Cybersécurité : Que faire une fois victimes de cyberattaque

Internet

Posté par : JerryG

Publié le : 8/12/2023 13:00:00

La France est le pays d'Europe qui a le plus faible taux d'adoption (37%) de cette technologie au sein des entreprises qui n'ont pas encore été victime de cyberattaque

Trellix, la spécialiste de la cybersécurité et pionnière dans la détection et la réponse étendue (XDR), dévoilait récemment le second volet de son étude baptisée « Mind of the CISO : Behind the Breach ».

Dans le cadre de ce rapport, elle a interrogé plus de 500 responsables de la sécurité des systèmes d'information travaillant dans des entreprises de plus de 1000 employés afin de mieux comprendre les défis auxquels ils sont confrontés après avoir subi une cyberattaque.

La France se distingue des autres pays d'Europe en ce que l'adoption de technologies avancées telles que le XDR n'intervient dans près d'un cas sur 2 (43%) qu'après avoir été victime d'une cyberattaque majeure.

Le manque de technologie de pointe comme première cybermenace

Interrogés sur la variable d'ajustement principale suite à une cyberattaque, 70% des RSSI européens s'attendent sur le fait que les améliorations à introduire portent sur la technologie ou les technologies cyber dont leurs entreprises sont équipées.

Particulièrement élevé en France, ce pourcentage s'élève à 80%, démontrant un besoin accru d'investissements dans des technologies plus avancées. Pour la presque majorité des responsables français (47%), la raison identifiée derrière une cyberattaque d'ampleur est celle d'une technologie qui n'était pas à la hauteur. Par opposition, la première raison invoquée par les RSSI anglais et allemands est l'incapacité à contenir rapidement, même après sa détection, un incident.

Les Français n'hésitent pas à opérer des changements majeurs après une cyberattaque

En France, une cyberattaque majeure conduit le plus souvent à une réévaluation complète de la stratégie cyber de l'entreprise tandis que dans le reste de l'Europe, elle a le plus souvent seulement pour conséquence l'achat de solutions de cybersécurité supplémentaires.

Synonyme de perturbations importantes pour les RSSI français, 47% d'entre eux déclarent qu'une cyberattaque majeure a engendré des interruptions d'activité, au sein de leur entreprise, soit le pourcentage le plus élevé d'Europe. A cela s'ajoute un stress supplémentaire important pour les équipes en charge de la cybersécurité.

Les entreprises françaises sont aussi plus susceptibles que leurs homologues européennes de changer de prestataire suite à une cyberattaque majeure (83% vs. 68% pour la moyenne européenne). En revanche, pour ceux qui n'envisagent pas de changer, c'est le coût qui est évoqué comme premier frein (80%).

Vers une adoption du XDR

Interrogés plus en détails sur les solutions technologiques dont ils disposaient avant vs. après une cyberattaque majeure, on constate que le taux d'adoption de certaines technologies clés telles que le XDR, le Endpoint ou le Threat Intelligence sont parmi les plus bas d'Europe en France (respectivement, 40%, 27% et 40%). 43% des entreprises françaises se sont finalement équipées du XDR suite à une cyberattaque, 60% du Endpoint et 47% de la Threat Intelligence, des pourcentages plus élevés que la moyenne européenne.

Parmi ceux qui n'avaient pas équipé une solution XDR, 80% des RSSI français estiment que cette technologie aurait pu leur offrir une meilleure compréhension du paysage cyber actuel et des menaces émergentes.

En outre, 58% pensent qu'il y aurait eu moins d'impact sur leur entreprise si le XDR avait été implémenté et 80% déclarent que cela aurait au moins pu leur permettre de prévenir la menace. Enfin, 93% des répondants français déclarent avoir obtenu plus de soutien de leur direction après une attaque.

« L'évolution rapide des cybermenaces couplée à la pénurie de ressources va obliger les organisations à basculer dans le SOC du futur dont la remédiation rapide est la pierre angulaire.

Le XDR s'impose aujourd'hui comme une approche à valeur ajoutée permettant d'obtenir cette visibilité indispensable à la mise en œuvre d'une réponse unifiée la plus rapide possible face à la complexité croissante des cybermenaces. Il reste toutefois beaucoup d'efforts à faire car la perception de la puissance du XDR reste plus faible en France que dans le reste de l'Europe », a déclaré Adrien Vandeweghe, Directeur France et Bénélux de Trellix.